EXHIBIT A

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

DEBORAH WESCH,

Plaintiff,

v.

YODLEE, INC., et al.,

Defendants.

Case No. 20-cv-05991-SK

ORDER REGARDING MOTIONS TO DISMISS

Regarding Docket Nos. 31, 32

This matter comes before the Court upon consideration of the motion to dismiss for failure to state a claim filed by Yodlee, Inc. ("Yodlee") and the motion to dismiss for lack of jurisdiction filed by Envestnet, Inc. ("Envestnet") (collectively, "Defendants"). Having carefully considered the parties' papers, relevant legal authority, and the record in the case, and having had the benefit of oral argument, the Court HEREBY GRANTS IN PART and DENIES IN PART Yodlee's motion and RESERVES RULING on Envestnet's motion for the reasons set forth below.

BACKGROUND

Plaintiffs Deborah Wesch, Darius Clark, John H. Cottrell, William B. Cottrell, Ryan Hamre, Greg Hertik, Daisy Hodson, David Lumb, Kyla Rollier and Jenny Szeto (collectively, "Plaintiffs") filed this purported class action against Yodlee and Envestnet to contest how Defendants access and treat the personal financial data of Plaintiffs and purported class members.

Plaintiffs allege that Yodlee surreptitiously collects such data from software products that it markets and sells to some of the large financial institutions, wealth management firms, and digital payment platforms like PayPal, which use Yodlee's software. (Dkt. No. 30 (First Amended Compl. ("FAC"), ¶ 4.). Yodlee then acquires individuals' financial data when those individuals interact with the software installed on these financial institutions' systems. (*Id.*, ¶ 5.) The financial institutions, such as PayPal, disclose to individuals that Yodlee is involved in connecting

their individual accounts to PayPal's service for the limited purpose of confirming the individuals' bank details, checking their balance, and transactions, as needed. However, Yodlee's collection of the individuals' data goes well beyond their limited consent provided to facilitate a connection between their bank accounts and PayPal. (*Id.*, ¶ 7.) For example, when individuals link their bank accounts to their PayPal account, they see the following message:

> We use Yodlee to confirm your bank details and to check your balance and transactions as needed, which can help your PayPal payments to through. For more information, see our Privacy Statement. You can turn off our use of Yodlee by removing permissions for this bank in your Profile.

(*Id.*, ¶ 55.) Then there is a button which states: "Agree and Link." (*Id.*) Individuals do not give PayPal or Yodlee permission to collect and store their financial information for resale. (*Id.*, ¶ 56.)

However, Yodlee goes beyond facilitating the log in transactions. Yodlee stores a copy of the individuals' banking data and retains their usernames and passwords for their financial institutions to collect and store the individuals' bank account transaction history on an ongoing basis. (*Id.*, ¶¶ 8, 9, 57.) The individuals did not consent to this kind of data collection, which is unrelated and unnecessary to complete their log in transactions. (*Id.*)

Despite the statement that individuals may turn off the use of Yodlee, individuals cannot opt out of or turn off Yodlee's access to their bank account information after providing their credentials. (*Id.*, ¶ 58.) Additionally, even if the individuals sever their connection with their financial institution, Yodlee continues to use the individuals' log in information to access their financial accounts. (*Id.*, ¶¶ 10, 58.)

Yodlee then aggregates the individuals' financial data and sells it to third parties. (*Id.*, ¶ 56.)

Plaintiffs allege that they suffered the following economic damages as a result of Yodlee's conduct:

> (a) the loss of valuable indemnification rights; (b) the loss of other rights and protections to which they were entitled as long as their sensitive personal data remained in a secure banking environment; (c) the loss of control over valuable property; and (d) the heightened risk of identity theft and fraud.

(*Id.*, ¶ 95.)

With respect to indemnity rights, Plaintiffs explain that, if someone uses an individual's credentials to log into a financial institution and improperly transfers funds, the individual would not be indemnified for the improperly transferred funds because the individual initially provided the credentials to Yodlee. (*Id.*, ¶¶ 97, 114.)

Plaintiffs have an expectation of privacy in their personal financial data, which Yodlee is collecting without their consent. (*Id.*, ¶ 100.) Additionally, even though Yodlee sold the individuals' data in an aggregated manner, the individuals could be identified using three months of transactions. (*Id.*, ¶¶ 110-113.)

Plaintiffs bring the following claims against Defendants: (1) invasion of privacy under both common law and the California Constitution; (2) violation of Stored Communication Act ("SCA"), 18 U.S.C. § 2701; (3) unjust enrichment; (4) violation of California Civil Code § 1709; (5) violation of California's Unfair Competition Law ("UCL"), California Business & Professions Code § 17200; (6) violation of California's Comprehensive Data Access and Fraud Act ("CDAFA"), California Penal Code § 502, (7) violation of California's Anti-Phishing Act of 2005, California Business & Professions Code § 22948.2, and (8) violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030.[1]

ANALYSIS

A. Applicable Legal Standard on Motion to Dismiss for Failure to State a Claim.

A motion to dismiss is proper under Federal Rule of Civil Procedure 12(b)(6) where the pleadings fail to state a claim upon which relief can be granted. On a motion to dismiss under Rule 12(b)(6), the Court construes the allegations in the complaint in the light most favorable to the non-moving party and takes as true all material allegations in the complaint. *Sanders v. Kennedy*, 794 F.2d 478, 481 (9th Cir. 1986). Even under the liberal pleading standard of Rule 8(a)(2), "a plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (citing *Papasan v. Allain*,

[1] Plaintiffs also brought a claim for declaratory relief, but agreed to withdraw this claim in response to Defendants' motion to dismiss. (Dkt. No. 37 at p. 25 n. 20.)

478 U.S. 265, 286 (1986)). Rather, a plaintiff must instead allege "enough facts to state a claim to relief that is plausible on its face." *Id.* at 570.

"The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully. . . . When a complaint pleads facts that are merely consistent with a defendant's liability, it stops short of the line between possibility and plausibility of entitlement to relief." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 557) (internal quotation marks omitted). If the allegations are insufficient to state a claim, a court should grant leave to amend, unless amendment would be futile. *See, e.g. Reddy v. Litton Indus., Inc.*, 912 F.2d 291, 296 (9th Cir. 1990); *Cook, Perkiss & Lieche, Inc. v. N. Cal. Collection Serv., Inc.*, 911 F.2d 242, 246-47 (9th Cir. 1990).

As a general rule, "a district court may not consider material beyond the pleadings in ruling on a Rule 12(b)(6) motion." *Branch v. Tunnell*, 14 F.3d 449, 453 (9th Cir. 1994), *overruled on other grounds, Galbraith v. Cnty. of Santa Clara*, 307 F.3d 1119 (9th Cir. 2002) (citation omitted). However, documents subject to judicial notice, such as matters of public record, may be considered on a motion to dismiss. *See Harris v. Cnty of Orange*, 682 F.3d 1126, 1132 (9th Cir. 2011). In doing so, the Court does not convert a motion to dismiss to one for summary judgment. *See Mack v. S. Bay Beer Distrib.*, 798 F.2d 1279, 1282 (9th Cir. 1986), *overruled on other grounds by Astoria Fed. Sav. & Loan Ass'n v. Solimino*, 501 U.S. 104 (1991). "The court need not . . . accept as true allegations that contradict matters properly subject to judicial notice . . . ." *Sprewell v. Golden State Warriors*, 266 F. 3d 979, 988 (9th Cir. 2001).

B. Yodlee's Motion to Dismiss.

Yodlee moves to dismiss all of Plaintiffs' claims. The Court will address each claim in turn.

1. Invasion of Privacy under the California Constitution and Common Law – Claims 1 and 10.

To state a claim for invasion of privacy based on the common law tort of intrusion, a plaintiff must allege: (1) that the defendant intentionally intruded into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy; and (2) the intrusion must

be highly offensive to a reasonable person. *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009). As the California Supreme Court explained, "the defendant must have 'penetrated some zone of physical or sensory privacy . . . or obtained unwanted access to data' by electronic or other covert means, in violation of the law or social norms." *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009) (quoting*Shulman v. Group W Productions, Inc.*, 18 Cal. 4th 200, 232 (1998)).

The right to privacy protected by the California Constitution is similar to the common law claim. *Hernandez*, 47 Cal. 4th at 287. To state a constitutional claim for invasion of privacy, a plaintiff must allege: (1) a legally protected privacy interest, such as conducting personal activities without observation, intrusion, or interference as determined by established social norms; (2) expectations of privacy which are reasonable; and (3) the intrusion must be so serious in nature, scope, and impact as to constitute an egregious breach of social norms. *Id*.

Yodlee argues that Plaintiffs do not have a reasonable expectation of privacy in anonymized, aggregated data. However, Plaintiffs allege that Yodlee improperly accessed and retained their personal, financial accounts at an individual level. Plaintiffs have a reasonable expectation of privacy in this data. Additionally, even though Yodlee sells this data in an aggregated manner, Plaintiffs allege that it would only take a few steps to identify the individual Plaintiffs from the transactions. (Dkt. No. 30, ¶¶ 110-113.) Therefore, the Court finds that Plaintiffs have sufficiently pled their invasion of privacy claims and DENIES Yodlee's motion to dismiss claims 1 and 10.

2. Stored Communications Act – Claim 2.

The Stored Communications Act prohibits any "person or entity providing an electronic communication service to the public" from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a). "[T]he Stored Communications Act protects individuals' privacy and proprietary interests. The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility." *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004). Yodlee argues that it (1) is not an electronic communication service; (2) does not access the contents of a communication; or (3) does not keep Plaintiffs' data

in electronic storage.

An electronic communication service ("ECS") is "any service which provides to its users the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). "[T]he statutory definitions of [electronic communication service] and [remote computing service] are functional and context sensitive." *Hately v. Watts*, 917 F.3d 770, 790 (4th Cir. 2019) (citation omitted). "[W]ebsites and services that permit users to communicate directly with one another are considered ECS providers." *Casillas v. Cypress Ins. Co.*, 770 F. App'x 329, 330 (9th Cir. 2019) (holding that a system enabling document uploads and downloads did not qualify as an ECS provider because it did not allow direct communication). Here, Plaintiffs allege that Yodlee provides "a service that allows Plaintiffs and Class members the ability to send and receive electronic communications from their financial institutions and third-party applications." (Dkt. No. 30, ¶ 162.) Therefore, Plaintiffs sufficiently allege that Yodlee is an ECS.

Next Yodlee argues that it does not access the "contents" of a "communication" under the statute because it merely accesses transactional data. Yodlee cites to cases which distinguish between the content or intended message and the information regarding the characteristics of the message generated in the course of the communication, such as header information or the webpage address. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106-07 (9th Cir. 2014); *see also Chevron Corp. v. Donziger*, 2013 WL 4536808, at *6 (N.D. Cal. Aug. 22, 2013) (distinguishing information about the email users, such as their name, email address, and IP address, from the content of the emails). However, here, the transactional data *is* the communication, as opposed to information about the person or entity sending the communication. Additionally, the transactional data includes sensitive financial records which reveal personal details of Plaintiffs' lives and their expenditures. Therefore, the Court finds that Plaintiffs sufficiently allege that Yodlee accesses the contents of a communication under the statute.

However, with respect to "electronic storage" under the SCA, the Court finds that Plaintiffs fail to allege facts sufficient to satisfy the statutory definition. The SCA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" or "any storage of such

communication by an electronic communication service for purposes of backup protection of such communication" 18 U.S.C.A. § 2510(17). Courts have held that communications stored for long periods, such as one year, do not qualify as "temporary, intermediate storage" under the first prong. *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1059 (N.D. Cal. 2012) (plaintiffs failed to allege "temporary, intermediate storage" where they alleged the data was stored for up to a one-year period); *In re Toys R Us, Inc., Privacy Litig.*, 2001 WL 34517252, at *3 (N.D. Cal. Oct. 9, 2001) (SCA "only protects electronic communications stored 'for a limited time' in the 'middle' of a transmission, i.e. when an electronic communication service temporarily stores a communication while waiting to deliver it."). As for the second prong, the storage must be "for purposes of backup protection." *KLA-Tencor Corp. v. Murphy*, 717 F. Supp. 2d 895, 904 (N.D. Cal. 2010) (citing *Theofel v. Farey-Jones,* 359 F.3d 1066, 1075-76 (9th Cir.2004)).

Here, although Plaintiffs allege that Yodlee stores their financial data, they do not allege that the storage is incidental to the electronic transmission of that data or that Yodlee's storage is temporary. Additionally, Plaintiffs do not allege that Yodlee stores its data for the purposes of providing backup protection for the communication between Plaintiffs and their financial institutions. Instead, Plaintiffs allege that Yodlee stores the information for its own misuse of the data. Therefore, the Court GRANTS Yodlee's motion to dismiss as to Plaintiffs' SCA claim, but with leave to amend.

3. Unjust Enrichment – Claim 3.

Yodlee argues that Plaintiffs fail to plead their unjust enrichment claim with sufficient particularity because it is grounded in fraud. Where a plaintiff alleges a claim grounded in fraud, Federal Rule of Civil Procedure 9(b) requires the plaintiff to state with particularity the circumstances constituting fraud, including the "who, what, when, where, and how" of the charged misconduct. *See Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1106 (9th Cir. 2003); *In re GlenFed, Inc. Sec. Litig.*, 42 F.3d 1541, 1547-49 (9th Cir. 1994). However, Rule 9(b) particularity requirements must be read in harmony with Federal Rule of Civil Procedure 8's requirement of a "short and plain" statement of the claim. Thus, the particularity requirement is satisfied if the complaint "identifies the circumstances constituting fraud so that a defendant can prepare an

adequate answer from the allegations." *Moore v. Kayport Package Exp., Inc.*, 885 F.2d 531, 540 (9th Cir. 1989).

However, a plaintiff pleading fraud by omission obviously cannot specify the time, place, and specific content of an omission. Therefore, fraud by omission claims do not require the same level of specificity required by a normal fraud claim. *See, e.g., Washington v. Baenziger*, 673 F. Supp. 1478, 1482 (N.D.Cal. 1987) ("Where the fraud consists of omissions on the part of the defendants, the plaintiff may find alternative ways to plead the particular circumstances of the fraud. [F]or example, a plaintiff cannot plead either the specific time of the omission or the place, as he is not alleging an act, but a failure to act.") (internal citations and quotations omitted); *see also MacDonald v. Ford Motor Co.*, 37 F. Supp. 3d 1087, 1096 (N.D. Cal. 2014) ("Because the plaintiffs are alleging a failure to act instead of an affirmative act, the Plaintiffs cannot point out the specific moment when the Defendant failed to act.") (quotation marks and brackets omitted).

Plaintiffs allege that Yodlee was unjustly enriched by surreptitiously acquiring their sensitive financial data through a fraudulent scheme and then selling subscriptions to that data for millions of dollars a year. (*Id.*, ¶¶ 46, 47, 48.) When individuals are prompted to enter their credentials to connect their bank accounts to PayPal, the log in screens mirrored what they would see if they were logging in directly to their respective banks. (*Id.*, ¶ 6.) Yodlee then stores a copy of those individuals' bank log in information and exploits that information to routinely extract financial data without individuals' knowledge or consent. (*Id.*, ¶¶ 8, 9.) Plaintiffs' allegations are sufficient to put Yodlee on notice of the substance of the alleged fraudulent scheme.

Yodlee also argues that Plaintiffs' claim must be dismissed because they fail to allege that they have an adequate remedy at law. However, Plaintiffs do make such an allegation. (Dkt. No. 30, ¶ 198.) Moreover, although Plaintiffs assert claims for legal remedies, Plaintiffs may plead in the alternative. Accordingly, the Court DENIES Yodlee's motion as to Plaintiffs' claim for unjust enrichment.

4. Cal. Civ. Code § 1709 – Claim 4.

California Civil Code section 1709 provides: "One who willfully deceives another with intent to induce him to alter his position to his injury or risk, is liable for any damage which he

thereby suffers." Cal. Civ. Code § 1709. Yodlee argues that Plaintiffs fails to allege the purported deceit with sufficient particularity. However, as discussed above, the Court finds that Plaintiffs sufficiently allege Yodlee's alleged fraudulent scheme to deceive Plaintiffs. Yodlee also argues that Plaintiffs fail to allege that they relied on any purported omission or that they suffered any damages. Upon review of the Amended Complaint, the Court finds that Plaintiffs have alleged sufficient facts to support their claim under Section 1709. Plaintiffs allege that, had they "known the true nature, significance and extent of Defendants' data practices, they would not have used Yodlee." (Dkt. No. 30, ¶ 94.) With respect to damages, as discussed above, Plaintiffs allege a loss of privacy to their financial data. Accordingly, the Court DENIES Yodlee's motion to dismiss as to Plaintiffs' claim under Section 1709.

5. Cal. UCL – Bus. & Prof. Code § 17200 – Claim 5.

To have standing to bring a claim under the UCL, Plaintiffs must have suffered an injury in fact and must have lost money or property as a result of the unfair competition. *See* Cal. Bus. & Prof. Code § 17204; *see also Californians for Disability Rights v. Mervyn's, LLC*, 39 Cal. 4th 223, 227 (2006). "To satisfy the narrower standing requirements imposed by Proposition 64, a party must now (1) establish a loss or deprivation of money or property sufficient to qualify as injury in fact, i.e., *economic injury*, and (2) show that the economic injury was the result of, i.e., *caused by*, the unfair business practice or false advertising that is the gravamen of the claim." *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 322 (2011) (emphasis in original).

Yodlee argues that Plaintiff have not alleged that they lost money or property as a result of Yodlee's alleged conduct. The Court agrees. First, Plaintiffs argue that they allege damages of "Loss of Benefit of the Bargain" by surrendering more or acquiring less in a transaction than they otherwise would have. (Dkt. No. 37 (citing *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 985 (N.D. Cal. 2016).) However, Plaintiffs have not alleged a transaction or contract *with Yodlee*, therefore, it is not clear how they alleged such damages. Second, Plaintiffs argue in reliance on *Romero v. Securus Techs., Inc.*, 216 F. Supp. 3d 1078, 1091 (S.D. Cal. 2016) that they alleged damages by alleging that they would not have used Yodlee if they knew the truth of its practices. The court in *Romero* held that the plaintiffs sufficiently alleged damages by alleging

that they would not have paid for and used the defendant's telephone system, or would not have paid as much for them, had they known about the defendant's fraud. *Id*. However, because Plaintiffs have not paid Yodlee any money and have not alleged that they paid PayPal any money for use of its service; Plaintiffs have not alleged how they lost money or property in this manner.

Third, Plaintiffs argue that they have lost valuable indemnification rights. Plaintiffs allege that, if a malicious person uses Plaintiffs' credentials to improperly transfer funds, banks would consider the transfer authorized because of Plaintiffs' initial provision of their credentials to Yodlee. Plaintiffs therefore would not be indemnified for the loss of transferred funds. (Dkt. No. 30, ¶ 97.) However, Plaintiffs have not alleged that anyone actually improperly transferred funds from their accounts. Therefore, any monetary loss at this point is merely potential or hypothetical. Fourth, Plaintiffs argue that Yodlee's conduct placed them at heightened risk of identity theft and fraud. However, again, Plaintiffs do not allege that any of them actually suffered identity theft or any actual monetary loss. Therefore, the Court finds that Plaintiffs have not alleged facts sufficient to establish standing required to bring a claim under the UCL. The Court thus grants Yodlee's motion as to this claim but will provide leave to amend.

6. Computer Fraud and Abuse Act and California Comprehensive Data Access and Fraud Act – Claims 7 and 9.

i. Loss or Damage.

Under both the Computer Fraud and Abuse Act ("CFAA), 18 U.S.C. § 1030 and the California Comprehensive Data Access and Fraud Act ("CDAFA"), Cal. Pen. Code § 502, Plaintiff must allege some damage or loss. *In re Google Android Consumer Priv. Litig.*, 2013 WL 1283236, at *6 (N.D. Cal. Mar. 26, 2013) (both "CFAA and CDAFA [c]laims require some showing of damage or loss, beyond the mere invasion of statutory rights").

The CFAA criminalizes accessing a computer without authorization or exceeding authorization. 18 U.S.C. § 1030(a). The statute also authorizes civil claims by individuals who suffered damage or loss of at least $5,000 as a result. 18 U.S.C. § 1030(c)(4)(A)(i); 18 U.S.C. § 1030(g). The statute defines loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program,

system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service[.]" 18 U.S.C. § 1030(e)(11). Plaintiffs allege in a conclusory fashion that they incurred "the cost of conducting damage assessments, restoring the data to its condition prior to the offense, and consequential damages they incurred by, inter alia, spending time conducting research to ensure that their identity had not been compromised and accounts reflect the proper balances" in excess of $5,000 per year. (Dkt. No. 30, ¶ 233.) The Court finds these conclusory allegations are insufficient and thus GRANTS Yodlee's motion to dismiss the CFAA claim with leave to amend.

Similarly, while the CDAFA does not set a minimum threshold, a plaintiff must allege that she is the "owner or lessee of the computer, computer system, computer network, computer program, or data" and must have suffered "damage or loss" to bring a civil claim. Cal. Penal Code § 502(e)(1). Although Plaintiffs allege that they owned the data, they fail to allege that the data incurred any damage or loss. Therefore, the Court GRANTS Yodlee's motion to dismiss the CDAFA with leave to amend.

Even though the Court is dismissing these claims on the grounds noted above, the Court provides guidance below on the other arguments because Plaintiffs may amend the CFAA and CDAFA claims.

ii. Unauthorized Access.

Both the CFAA and the CDAFA prohibit unauthorized access to a computer system. Yodlee argues that Plaintiffs provided consent and therefore its access was not unauthorized. Under the CFAA, the statute defines "exceeds authorized access" to mean accessing "a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled *so* to obtain or alter." *United States v. Nosal*, 642 F.3d 781, 785 (9th Cir. 2011) (emphasis in original) (quoting § 1030(e)(6)); *Musacchio v. United States*, 136 S. Ct. 709, 713 (2016) ("exceeds authorized access" means "obtaining access with authorization but then using that access improperly"). Here, Plaintiffs allege that Yodlee exceeded its authorization to access their data. They allege that Yodlee stores their login information to their financial institutions and accesses their account transaction history on an ongoing basis, *unrelated* to

facilitating their transactions with PayPal. (Dkt. No. 30. ¶¶ 10, 56-58.) Such allegations are sufficient to allege access which exceeds Yodlee's authorization.

iii. Damage to a Computer.

Certain provisions of the CFAA and CDAFA require "damage" to the data or computer system and not merely loss. Section 1030(a)(5)(A) of the CFAA requires a showing that a defendant intentionally caused "damage" without authorization to a protected computer. 18 U.S.C. § 1030(a)(5)(A); *see also see* 18 U.S.C. § 1030(e)(8) (defining "damage" as "any impairment to the integrity or availability of data, a program, system, or information"). Similarly, section 502(c)(4) of the CDAFA requires a showing that a defendant "adds, alters, damages, deletes, or destroys any data." Cal. Pen. Code § 502(c)(4).[2] The Court finds that Plaintiffs fail to allege that any data or computer system was actually damaged. Plaintiffs cite to *Therapeutic Research Faculty v. NBTY, Inc.*, 488 F. Supp. 2d 991, 996 (E.D. Cal. 2007) for the proposition that the "alleged unauthorized access to the Publication and the disclosure of its information may constitute an impairment to the integrity of data or information even though 'no data was physically changed or erased.'" However, the only case *Therapeutic Research* cites to is a case which addresses the disclosure of *trade secrets* which, by their nature, are damaged by their disclosure. *See Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F.Supp.2d 1121, 1126 (W.D.Wash.2000) (stating "the alleged access and disclosure of trade secrets" constituted an "impairment to the integrity of data . . . or information."). Therefore, the Court finds that *Therapeutic Research* is not persuasive. If Plaintiffs elect to amend their claims under Section 1030(a)(5)(A) of the CFAA and Section 502(c)(4) of the CDAFA, Plaintiffs shall allege that their data was damaged.

iv. Intent to Defraud.

Sections 1030(a)(4) and 1030(a)(6) required a showing of "knowingly and with intent to defraud." *See* 18 U.S.C. §§ 1030(a)(4), (6). Yodlee argues that Plaintiffs fail to allege fraud with

[2] Yodlee also points to Section 502(c)(1) of the CDAFA as requiring damage, but that provision states "damages, deletes, destroys, or *otherwise uses* any data." Cal. Pen. Code § 502(c)(1) (emphasis added).

sufficient particularity. However, as discussed above, the Court finds that Plaintiffs have sufficiently alleged a fraudulent scheme.

v. Traffics any Password as required under 18 U.S.C. § 1030(a)(6)

Section 1030(a)(6) of the CFAA prohibits a defendant from "traffic[ing] . . . in any password or similar information through which a computer may be accessed without authorization. . . ." *See* 18 U.S.C. § 1030(a)(6). The term "traffic" means "transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of." 18 U.S.C. § 1029(e)(5). Plaintiffs allege that Yodlee *used* Plaintiffs passwords and sold Plaintiff's financial data, but do not allege that Yodlee *trafficked* (transferred, or otherwise disposed of, to another) Plaintiffs' passwords. Therefore, Plaintiffs' claim under Section 1030(a)(6) is deficient for this additional reason. However, the Court will provide Plaintiffs with leave to amend.

7. California Anti-Phishing Act of 2005 – Claim 8.

The California Anti-Phishing Act of 2005, California Business and Professions Code § 22948.2, prohibits use of the internet to "solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business." Cal. Bus. & Prof. Code § 22948.2. "Identifying information" includes a "[b]ank account number," "[a]ccount password," and "[a]ny other piece of information that can be used to access an individual's financial accounts . . . ." *Id.* § 22948.1(b). Plaintiffs allege:

> Defendants violated the Anti-Phishing Act by representing themselves to be Plaintiffs' and Class members' financial institutions. Defendants fraudulently and deceitfully impersonated those institutions in order to induce Plaintiffs and Class members to provide their login credentials to Defendants, as described herein. Defendants did so without obtaining the authority or approval of each financial institution.

(Dkt. No. 30, ¶ 216.) These allegations are sufficient to state a claim under the California Anti-Phishing Act. Therefore, the Court DENIES Yodlee's motion to dismiss this claim.

C. Legal Standards on Motion to Dismiss for Lack of Jurisdiction.

When a defendant moves to dismiss for lack of subject matter jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1), the plaintiff bears the burden of proving that the court

has jurisdiction to decide the claim. *Thornhill Publ'n Co. v. Gen. Tel. & Elecs. Corp.*, 594 F.2d 730, 733 (9th Cir. 1979). Federal courts can only adjudicate cases which the Constitution or Congress authorize them to adjudicate: cases involving diversity of citizenship, or those cases involving a federal question, or where the United States is a party. *See, e.g., Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994).

A Rule 12(b)(1) motion can be either "facial" or "factual." *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). Where an attack on jurisdiction is a "facial" attack on the allegations of the complaint, the factual allegations of the complaint are taken as true and the non-moving party is entitled to have those facts construed in the light most favorable to him or her. *Federation of African Am. Contractors v. City of Oakland*, 96 F.3d 1204, 1207 (9th Cir. 1996).

In a "factual attack," the moving party questions the veracity of the plaintiff's allegations that "would otherwise invoke federal jurisdiction." *Safe Air for Everyone*, 373 F.3d at 1039. The plaintiff's allegations are questioned by "introducing evidence outside the pleadings." *Leite v. Crane Co.*, 749 F.3d 1117, 1121 (9th Cir. 2014). "When the defendant raises a factual attack, the plaintiff must support her jurisdictional allegations with 'competent proof,' under the same evidentiary standard that governs in the summary judgment context." *Id.* (quoting *Hertz Corp. v. Friend*, 559 U.S. 77, 96-97 (2010)). While the plaintiff typically has the burden of proof to establish subject matter jurisdiction, "if the existence of jurisdiction turns on disputed factual issues, the district court may resolve those factual disputes itself." *Id.* at 1121-22 (citing *Safe Air for Everyone*, 373 F.3d at 1039-40).

D. Envestnet's Motion to Dismiss.

Envestnet moves to dismiss on the grounds that Plaintiffs fail to allege any misconduct by it, but instead, seeks to hold Envestnet liable for Yodlee's conduct. Envestnet argues that Plaintiffs have not alleged sufficient facts to hold Envestnet liable under an *alter ego* theory.

While there is no "litmus test" for *alter ego* liability, there are "two general requirements: (1) that there be such unity of interest and ownership that the separate personalities of the corporation and the individual no longer exist and (2) that, if the acts are treated as those of the corporation alone, an inequitable result will follow." *Mesler v. Bragg Mgmt. Co.*, 39 Cal. 3d 290,

300 (1985) (citations omitted). "*Alter ego* is an extreme remedy, sparingly used." *Sonora Diamond Corp. v. Sup. Ct.*, 83 Cal. App. 4th 523, 539 (2000); *see also Katzir's Floor & Home Design, Inc. v. M-MLS.com*, 394 F.3d 1143, 1149 (9th Cir. 2004) (quoting *Dole Food Co. v. Patrickson*, 538 U.S. 468, 475 (2003) ("The doctrine of piercing the corporate veil, however, is the rare exception, applied in the case of fraud or certain other exceptional circumstances."). It may be "invoked only where recognition of the corporate form would work an *injustice* to a third person." *Tomaselli v. Transamerica Ins. Co.*, 25 Cal. App. 4th 1269, 1285 (1994) (emphasis in original) (noting that "inadequate capitalization, commingling of assets, disregard of corporate formalities" are "critical facts" to show an inequitable result would follow). "[W]hile the doctrine does not depend on the presence of actual fraud, it is designed to prevent what would be fraud or injustice, if accomplished." *Assoc. Vendors, Inc. v. Oakland Meat Co.*, 210 Cal.App.2d 825, 838 (1962). "Accordingly, bad faith in one form or another is an underlying consideration." *Id.*

The Court may rely on the following factors to establish a unity of interest: commingling of funds, identification of the equitable owners with domination and control of the two entities, instrumentality or conduit for a single venture or the business of an individual, failure to maintain minutes or adequate corporate records, use of the same office or business locations, identical equitable ownership of the two entities, use of a corporation as a mere shell, and the failure to adequately capitalize a corporation. *Id*. Some courts have held that the pleading of at least two factors in support of a unity of interest satisfies this element. *See Pacific Maritime Freight, Inc. v. Foster*, 2010 WL 3339432, at *6 (S.D. Cal. Aug. 24, 2010) (citing authority that the identification of unity of interest for alter ego liability plus two or three factors was held sufficient to defeat a motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6)) (internal citations omitted.

"California courts generally require evidence of some bad-faith conduct to fulfill the second prong of alter-ego liability, [and] that bad faith must make it inequitable to recognize the corporate form." *Smith v. Simmons*, 638 F. Supp. 2d 1180, 1192 (E.D. Cal. June 23, 2009) (noting that California courts generally require some evidence of bad faith before concluding that an inequitable result justifies an alter ego finding); *see also Associated Vendors, Inc. v. Oakland Meat*

Co., 210 Cal. App. 2d 825, 842 (1962) ("The purpose of the doctrine is not to protect every unsatisfied creditor, but rather to afford him protection, where some conduct amounting to bad faith makes it inequitable . . . for the equitable owner of a corporation to hide behind its corporate veil.

Here, Plaintiffs have not yet alleged sufficient facts to proceed on their *alter ego* theory. However, the Court will provide Plaintiffs with a limited time period to conduct discovery on this issue. Therefore, the Court RESERVES RULING on Envestnet's motion to dismiss pending this discovery. The Court ORDERS that Plaintiffs may issue five document requests, five interrogatories, and five requests for admission on this subject and take one deposition of Envestnet pursuant to Fed.R.Civ.P. 60(b)(6). After conducting such discovery, by no later than May 28, 2021, Plaintiffs shall file a supplemental brief with their supporting evidence to demonstrate personal jurisdiction over Envestnet. Envestnet may file a supplemental response brief by no later than June 11, 2021.

CONCLUSION

For the foregoing reasons, the Court GRANTS IN PART and DENIES IN PART Yodlee's motion to dismiss and RESERVES RULING on Envestnet's motion to dismiss. The Court GRANTS Yodlee's motion as to Plaintiffs' claims under the Stored Communications Act claim, the UCL, the CFAA, and the CDAFA, and DENIES Yodlee's motion as to the remainder of Plaintiffs' claims. By no later than March 15, 2021, Plaintiffs may file an amended complaint to cure the deficiencies addressed in this Order.

The Court STAYS all discovery against any defendant other than the limited discovery regarding jurisdiction.

IT IS SO ORDERED.

Dated: February 16, 2021

SALLIE KIM
United States Magistrate Judge

United States District Court
Northern District of California